# ある代数曲線上の点のなす群(モデル理論における独立概念と次元)

AUTHOR(S):

田中, 克己

CITATION:

田中, 克己. ある代数曲線上の点のなす群(モデル理論における独立概念と次元). 数理解析研究所講究録 2007, 1555: 30-39

ISSUE DATE:

2007-05

URL:

http://hdl.handle.net/2433/80990

数理解析研究所講究録
第1555巻 2007年 30-39



# ある代数曲線上の点のなす群

岡山大学理学部数学教室・田中　克己 (Katsumi Tanaka)
Department of Mathematics, Okayama University

平成19年2月28日

## 1　ペルの方程式

このノートでは、

$$x^2 - dy^2 = 1 \tag{1}$$

の形をした2元2次方程式の整数解について考える。ここで、$d$ は正の整数で、平方数ではないとする。

整数解 $(x,y)$ の全体を $G$ とおく。$G$ の元 $(x_1,y_1)$ と $(x_2,y_2)$ に対し、

$$(x_1,y_1) * (x_2,y_2) = (x_1x_2 + dy_1y_2, x_1y_2 + x_2y_1) \tag{2}$$

と定める。このとき、

- $G$ はアーベル群。
- $(1,0)$ は単位元。
- $(x,y)^{-1} = (x,-y)$。

という性質を持つことが知られている。それぞれチェックするのは簡単だが、$G$ が $*$ について閉じていることを示しておこう。

$$\begin{aligned}(x_1x_2 + dy_1y_2)^2 &= x_1^2x_2^2 + 2dx_1x_2y_1y_2 + d^2y_1^2y_2^2 - d(x_1^2y_2^2 + 2x_1x_2y_1y_2 + x_2^2y_1^2)\\ &= x_1^2x_2^2 - dx_1^2y_2^2 + d^2y_1^2y_2^2 - dx_2^2y_1^2\\ &= x_1^2(x_2^2 - dy_2^2) - dy_1^2(x_2^2 - dy_2^2)\\ &= (x_1^2 - dy_1^2)(x_2^2 - dy_2^2)\\ &= 1 \times 1\\ &= 1\end{aligned}$$

**例 1** $d = 2$ のとき、$x^2 - 2y^2 = 1$ は整数解 $(3,2)$ を持つ。さらに、$(3,2)^2 = (17,12), (3,2)^3 = (99,70), (577,408), (3363,2378), \cdots$ は整数解になる。

ここで、整数解以外についても次のことがいえる。

**命題 2** $\{(x,y) \in \mathbf{R} \times \mathbf{R} | x^2 - dy^2 = 1\}$ は演算 $*$ について群をなす。

群 $(G,*)$ はアーベル群なので、モデル論的にはその理論は安定である。したがって、群の言語では $G$ ないし $G^n$ 上に不安定な環（体）は解釈されない。

# 2 非自明解があれば解は無限個

## 2.1 $\sqrt{2}$ の連分数展開

この節では、$\sqrt{2}$ の無限連分数を考える。

$$(\sqrt{2}-1)(\sqrt{2}+1)=2-1=1 \tag{3}$$

よって、

$$\begin{aligned}\sqrt{2}-1 &= \frac{1}{\sqrt{2}+1}\\ &= \frac{1}{2+(\sqrt{2}-1)}\\ &= \frac{1}{2+\dfrac{1}{\sqrt{2}+1}}\\ &= \frac{1}{2+\dfrac{1}{2+(\sqrt{2}-1)}}\end{aligned}$$

したがって、

$$\sqrt{2}=1+\frac{1}{2+\dfrac{1}{2+(\sqrt{2}-1)}} \tag{4}$$

( ) の部分を次々と置き換えると、

$$\sqrt{2}=1+\frac{1}{2+\dfrac{1}{2+\dfrac{1}{2+\cdots}}} \tag{5}$$

一般に、

$$(\sqrt{m^2+1}-m)(\sqrt{m^2+1}+m)=1$$

であるから、$A=m^2+1$ とおけば、$\sqrt{A}$ を無限連分数に展開できる。

## 2.2 展開法

(5) に対する近似列 $\delta_1, \delta_2, \delta_3 \cdots$ を次のように定義する。

$$\begin{aligned}\delta_1 &= 1\\ \delta_2 &= 1+\frac{1}{2}=\frac{3}{2}\\ \delta_3 &= 1+\frac{1}{2+\dfrac{1}{2}}=\frac{7}{5}\\ \delta_4 &= 1+\frac{1}{2+\dfrac{1}{2+\dfrac{1}{2}}}=\frac{17}{12}\end{aligned}$$

以下、同様に $\delta_5, \delta_6, \cdots$ とおく。このとき、

$$\delta_1 < \delta_3 < \delta_5 < \cdots < \sqrt{2} < \cdots < \delta_6 < \delta_4 < \delta_2$$

が成り立つことは簡単に確かめることができる。

一般に、無理数 $\alpha$ の無限連分数展開

$$\alpha = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cfrac{1}{q_4 + \cdots}}}$$

に対して、

$$\delta_1 < \delta_3 < \cdots < \delta_{2n+1} < \cdots < \alpha < \cdots < \delta_{2n} < \cdots < \delta_4 < \delta_2 \quad 。$$

ここで、

$$\delta_k = \frac{P_k}{Q_k}$$

とおくと、

$$\begin{cases} P_k = P_{k-1}q_k + P_{k-2} \\ Q_k = Q_{k-1}q_k + Q_{k-2} \end{cases} \tag{6}$$

何故ならば、

$$\delta_1 = q_1 = \frac{P_1}{Q_1}, Q_1 = 1, p_1 = q_1$$

$$\delta_2 = q_1 + \frac{1}{q_2} = \frac{P_2}{Q_2} = \frac{q_1q_2+1}{q_2}, Q_2 = q_2, P_2 = q_1q_2 + 1$$

$$\delta_3 = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3}} = q_1 + \cfrac{1}{\cfrac{q_2q_3+1}{q_3}} = q_1 + \frac{q_3}{q_2q_3+1} = \frac{q_1q_2q_3 + q_1 + q_3}{q_2q_3+1}$$

したがって、

$$\begin{aligned} P_3 &= q_1q_2q_3 + q_1 + q_3 = (q_1q_2+1)q_3 + q_1 = P_2q_3 + P_1 \\ Q_3 &= q_2q_3 + 1 = Q_2q_3 + Q_1 \end{aligned}$$

次に (6) を帰納法で示す。

$k = 3$ のとき、上で OK。

$k = n$ のとき、成立すると仮定する。

$$\delta_n = \frac{P_n}{Q_n} = \frac{P_{n-1}q_n + P_{n-2}}{Q_{n-1}q_n + Q_{n-2}}$$

いま、$q_n$ を $\left(q_n + \dfrac{1}{q_{n+1}}\right)$ で置き換えれば $\delta_{n+1}$ になる。そこで、

$$\delta_{n+1} = \frac{P_{n-1}\left(q_n + \dfrac{1}{q_{n+1}}\right) + P_{n-2}}{Q_{n-1}\left(q_n + \dfrac{1}{q_{n+1}}\right) + Q_{n-2}}$$

$$
\begin{aligned}
&= \frac{P_n + \dfrac{1}{q_{n+1}} P_{n-1}}{Q_n + \dfrac{1}{q_{n+1}} Q_{n-1}} \\
&= \frac{P_n q_{n+1} + P_{n-1}}{Q_n q_{n+1} + Q_{n-1}} \\
&= \frac{P_{n+1}}{Q_{n+1}}
\end{aligned}
$$

**補題 3** $\delta_k - \delta_{k-1} = \dfrac{(-1)^k}{Q_k Q_{k-1}}$

**証明** $k=2$ のとき、$\delta_2 - \delta_1 = \dfrac{1}{q_2} = \dfrac{(-1)^2}{Q_2 Q_1}$ でOK。
$k=n$ のとき成立すると仮定する。
$k=n+1$ のとき、

$$\delta_{n+1} - \delta_n = \frac{P_{n+1}}{Q_{n+1}} - \frac{P_n}{Q_n} = \frac{P_{n+1}Q_n - P_n Q_{n+1}}{Q_{n+1}Q_n}$$

ここで、

$$
\begin{aligned}
\text{分子} &= (P_n q_{n+1} + P_{n-1})Q_n - P_n(Q_n q_{n+1} + Q_{n-1}) \\
&= P_n Q_n q_{n+1} + P_{n-1}Q_n - P_n Q_n q_{n+1} - P_n Q_{n-1} \\
&= P_{n-1}Q_n - P_n Q_{n-1} = -(P_n Q_{n-1} - P_{n-1}Q_n) \\
&= (-1)^{n-1}(P_2 Q_1 - P_1 Q_2) \\
&= (-1)^{n-1}(q_1 q_2 + 1 - q_1 q_2) \\
&= (-1)^{n+1} \qquad \square
\end{aligned}
$$

このことから、

$$
\begin{aligned}
\delta_{2k} - \delta_{2k+1} &= -(\delta_{2k+1} - \delta_{2k}) \\
&= \frac{(-1)^{2k}}{Q_{2k+1}Q_{2k}} = \frac{1}{Q_{2k+1}Q_{2k}}
\end{aligned}
$$

**補題 4** $0 < P_{2k} - \alpha Q_{2k} < \dfrac{1}{Q_{2k+1}}$

**証明** $\alpha < \delta_{2k} = \dfrac{P_{2k}}{Q_{2k}}$ より、$\alpha Q_{2k} < P_{2k}$。
よって、

$$0 < P_{2k} - \alpha Q_{2k}$$

また、$\delta_{2k+1} < \alpha < \delta_{2k}$ より、

$$
\begin{aligned}
\delta_{2k} - \alpha &< \delta_{2k} - \delta_{2k+1} = \frac{1}{Q_{2k}Q_{2k+1}} \\
\frac{P_{2k}}{Q_{2k}} - \alpha &< \frac{1}{Q_{2k}Q_{2k+1}}
\end{aligned}
$$

両辺に $Q_{2k}$ を掛けて、

$$P_{2k} - \alpha Q_{2k} < \frac{1}{Q_{2k+1}} \qquad \square$$

## 2.3 方程式 $x^2 - 2y^2 = 1$ の解

方程式 $x^2 - 2y^2 = 1$ について考える。

$$(x - \sqrt{2}y)(x + \sqrt{2}y) = x^2 - 2y^2$$

ここで、$x = P_{2k}$、$y = Q_{2k}$ とおくと、

$$(P_{2k} - \sqrt{2}Q_{2k})(P_{2k} + \sqrt{2}Q_{2k}) = P_{2k}^2 - 2Q_{2k}^2 \tag{7}$$

右辺は整数だから、左辺も整数。先の補題より、

$$0 < P_{2k} - \sqrt{2}Q_{2k} < \frac{1}{Q_{2k+1}}$$

(7) の左辺は正だから、

$$0 < P_{2k}^2 - 2Q_{2k}^2$$

また、

$$\begin{aligned} 0 < P_{2k} - \sqrt{2}Q_{2k} < \frac{1}{Q_{2k+1}} &= \frac{1}{Q_{2k}q_{2k+1} + Q_{2k-1}} \\ &\leq \frac{1}{2Q_{2k} + Q_{2k-1}} < \frac{1}{2Q_{2k}} \end{aligned}$$

ところが、

$$\delta_{2k} = \frac{P_{2k}}{Q_{2k}} > \sqrt{2}$$

だから、$\sqrt{2}Q_{2k} < P_{2k}$ となる。よって、

$$\begin{aligned} P_{2k} + \sqrt{2}Q_{2k} &< 2P_{2k} \\ P_{2k}^2 - Q_{2k}^2 &< \frac{2P_{2k}}{2Q_{2k}} = \frac{P_{2k}}{Q_{2k}} = \delta_{2k} \end{aligned}$$

ここで、

$$P_{2k} < \sqrt{2}Q_{2k} + \frac{1}{Q_{2k+1}}$$

より、

$$P_{2k}^2 - 2Q_{2k}^2 < \frac{P_{2k}}{Q_{2k}} < \frac{\sqrt{2}Q_{2k} + \dfrac{1}{Q_{2k+1}}}{Q_{2k}} = \sqrt{2} + \frac{1}{Q_{2k}Q_{2k+1}}$$

$k \geq 1$ に対して、

$$\frac{1}{Q_{2k}Q_{2k+1}} \leq \frac{1}{Q_2Q_3} = \frac{1}{2 \cdot 5} = \frac{1}{10}$$

よって、

$$P_{2k}^2 - 2Q_{2k}^2 < 2$$

したがって、

$$0 < P_{2k}^2 - 2Q_{2k}^2 < 2, \quad \forall k \geq 1$$

$P_{2k}^2 - 2Q_{2k}^2$ は整数だから、

$$P_{2k}^2 - 2Q_{2k}^2 = 1$$

以上より、次の命題を得る。

**命題 5** $(x, y) = (P_{2k}, Q_{2k})$ は方程式 $x^2 - 2y^2 = 1$ の解となる。

## 2.4 最小解

一般に $d > 1$ が平方数でない整数のとき、方程式 $x^2 - dy^2 = 1$ の整数解 $x$、$y$ を求める。$(x, y) = (1, 0)$ が解になるのは明らかなので、これを自明解とよぶことにする。上の方程式が自明でない整数解 $(a, b), a > 0, b > 0$ を持つと仮定する。

正の整数解 $(x, y)$ に対し、$x + y\sqrt{d}$ の値が最小のものをこの方程式の**最小解**という。方程式 $d = 2$ のときは、$(x, y) = (3, 2)$ が最小解である。

**補題 6** 最小解は存在すればただ一つである。

**証明** $(s, t), (u, v)$ を最小解とする。

$$s + t\sqrt{d} = u + v\sqrt{d}$$

ここで $s, t, u, v$ は整数、$\sqrt{d}$ は無理数だから、

$$s = u, \quad t = v \quad 。 \quad \square$$

次に方程式 (1) の重要な性質を示す。$(x_1, y_1)$ を方程式 (1) の解とすると、

$$x_1^2 - dy_1^2 = 1$$

したがって、

$$(x_1 + \sqrt{d}y_1)(x_1 - \sqrt{d}y_1) = 1 \tag{8}$$

となる。この式の両辺を $n$ 乗して、

$$(x_1 + \sqrt{d}y_1)^n(x_1 - \sqrt{d}y_1)^n = 1 \tag{9}$$

を得る。2 項定理より、

$$(x_1 + \sqrt{d}y_1)^n = x_1^2 + nx_1^{n-1} + \frac{n(n-1)}{2}x_1^{n-2}dy_1^2 + \cdots + (\sqrt{d})^n y_1^n \tag{10}$$

これを整理して、$x_n + \sqrt{d}y_n$ と書くことにする。このとき $x_n, y_n$ も整数になり、

$$(x_1 - \sqrt{d}y_1)^n = x_n - \sqrt{d}y_n$$

となる。

**補題 7** $(x_n, y_n)$ は方程式 (1) の解になる。

**証明**

$$\begin{aligned}(x_1 + \sqrt{d}y_1)^n(x_1 - \sqrt{d}y_1)^n &= (x_n + \sqrt{d}y_n)(x_n - \sqrt{d}y_n) \\ &= x_n^2 - dy_n^2 = 1\end{aligned}$$

**定理 8** 平方数でない正の整数 $d$ に対し、方程式

$$x^2 - dy^2 = 1$$

のすべての解は、$(\pm x_n, \pm y_n)$ の形をしている。ただし、

$$\begin{aligned}x_n &= \frac{1}{2}\{(a + b\sqrt{d})^n + (a - b\sqrt{d})^n\} \\ y_n &= \frac{1}{2\sqrt{d}}\{(a + b\sqrt{d})^n + (a - b\sqrt{d})^n\}\end{aligned}$$

**証明**この方程式の正の整数解 $(x', y')$ が存在して、どの自然数 $n$ に対しても、

$$x' + \sqrt{d}y' \neq (a + \sqrt{d}b)^n$$

とする。このとき、ある自然数 $n$ が存在して、

$$(a + b\sqrt{d})^n < x' + \sqrt{d}y' < (a + b\sqrt{d})^{n+1} \tag{11}$$

となる。$a + b\sqrt{d} > 0$ だから、式 (11) に $(a + b\sqrt{d})^n$ を掛けると、

$$1 < (x' + \sqrt{d}y')(a - b\sqrt{d})^n < a + b\sqrt{d}$$

となる。ここで、

$$\begin{aligned}(x' + \sqrt{d}y')(a - b\sqrt{d})^n &= (x' + \sqrt{d}y')(x_n - \sqrt{d}y_n) \\ &= x'x_n - dy'y_n + \sqrt{d}(y'x_n - x'y_n)\end{aligned}$$

これを $\bar{x} + \bar{y}\sqrt{d}$ とおく。このとき $\bar{x}$ と $\bar{y}$ は整数。$(\bar{x}, \bar{y})$ は方程式 (1) の解になる。

## 3 非自明解の存在

この節では、方程式

$$x^2 - dy^2 = 1$$

が自明でない整数解を持つことを示す。

**補題 9** $d$ が非平方数である正の整数のとき、ある自然数 $k$ が存在して、方程式

$$x^2 - dy^2 = k \tag{12}$$

が無限組の整数解をもつ。

**証明** 任意の正の実数 $\alpha$ の無限連分数展開を考える。

$$\alpha = [\alpha] + \{\alpha\}$$

と分解する。ここで、$[*]$ はガウス記号、$\{\alpha\}$ は $\alpha$ の小数部分。

$$[\alpha] = q_1, \{\alpha\} = \frac{1}{\alpha_1}$$

とおくと、

$$\alpha = q_1 + \frac{1}{\alpha_1}$$

ここで、$\alpha_1 > 1$ となる。これを繰り返して次の式を得る。

$$\begin{aligned}\alpha &= q_1 + \frac{1}{\alpha_1} \\ \alpha_1 &= q_2 + \frac{1}{\alpha_2}, q_2 = [\alpha_1] \\ &\vdots \\ \alpha_n &= q_{n+1} + \frac{1}{\alpha_{n+1}}, q_{n+1} = [\alpha_n] \\ &\vdots\end{aligned}$$

これより無限連分数展開、

$$\alpha = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cfrac{1}{q_4 + \cdots}}}$$

を得る。ここで、前節と同様に近似分数を

$$\begin{aligned} \delta_1 &= q_1 \\ \delta_2 &= q_1 + \frac{1}{q_2} \\ \delta_3 &= q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3}} \\ &\vdots \end{aligned}$$

とおいたとき、各 $k$ に対し、

$$\delta_k = \frac{P_k}{Q_k}$$

とおく。

無理数 $\alpha = \sqrt{d}$ の近似分数を使って、

$$P_{2n}^2 - dQ_{2n}^2 = (P_{2n} - \alpha Q_{2n})(P_{2n} + \alpha Q_{2n})$$

となり、この値を $z_{2n}$ と記す。ここで、

$$0 < P_{2n} - \alpha Q_{2n} < \frac{1}{Q_{2n+1}}$$

であるから、

$$0 < P_{2n} + \alpha Q_{2n} < 2\alpha Q_{2n} + P_{2n} - \alpha Q_{2n} < 2\alpha Q_{2n} + \frac{1}{Q_{2n+1}}$$

となる。$z_{2n}$ を評価すると、

$$0 < z_{2n} < \frac{1}{Q_{2n}}\left(2\alpha Q_{2n} + \frac{1}{Q_{2n+1}}\right) < 2\alpha + 1$$

となり、$z_{2n}$ は正の整数となる。1 と $2\alpha + 1$ の間には $[2\alpha + 1]$ 個の整数しかないから、ある $1 \leq k \leq [2\alpha + 1]$ が存在して、方程式 (12) は無限個の整数解を持つ。 □

方程式 (12) の無限個の解を $(u_n, v_n)_{n\in\omega}$ とリストすることにする。

**主張** $k = 1$

いま $k > 1$ と仮定する。つまり、方程式 (1) に非自明な解は無いと仮定する。各 $n \in \omega$ に対し、整数の組 $(u_n, v_n)$ のそれぞれの数を $k$ で割った余りを $p_n, q_n$ とする。余りの組 $(p_n, q_n)$ は有限（高々 $k^2$）の組合せしかありえない。鳩ノ巣論法により、少なくとも一つの組が無限回現われる。それを $(p, q)$ と表す。余りの組が $(p, q)$ となる方程式 (12) の解のリストを $(s_n, t_n)_{n\in\omega}$ とおく。ここで、$(s_n, t_n)$ は近似分数の分子と分母の組だから互いに素である。(6) より、

$$Q_2 < Q_4 < Q_6 < \cdots$$

よって、これらの部分列である $t_1, t_2, t_3, \cdots$ も互いに異なる。したがって、分数の列 $\frac{s_n}{t_n}$ もすべて異なる。

定義により、

$$s_1^2 - dt_1^2 = (s_1 - \alpha t_1)(s_1 + \alpha t_1) = k \tag{13}$$

$$s_2^2 - dt_2^2 = (s_2 - \alpha t_2)(s_2 + \alpha t_2) = k \tag{14}$$

ここで、$\alpha = \sqrt{d}$ だから、

$$(s_1 - \alpha t_1)(s_2 + \alpha t_2) = s_1 s_2 - dt_1 t_2 - \alpha(s_1 t_2 - s_2 t_1) \tag{15}$$

同様に、

$$(s_1 + \alpha t_1)(s_2 - \alpha t_2) = s_1 s_2 - dt_1 t_2 + \alpha(s_1 t_2 - s_2 t_1) \tag{16}$$

ここで、$(s_n, t_n)$ の性質より、

$$s_n = a_n k + p, \quad t_n = b_n + q$$

と表せる。このとき、

$$\begin{aligned} s_1 s_2 - dt_1 t_2 &= s_1(a_2 k + p) - dt_1(b_2 k + q) \\ &= s_1\{(a_2 - a_1)k + a_1 k + p\} - dt_1\{(b_2 - b_1)k + b_1 k + q\} \\ &= s_1\{(a_2 - a_1)k + s_1\} - dt_1\{(b_2 - b_1)k + t_1\} \\ &= k\{s_1(a_2 - a_1) - dt_1(b_2 - b_1)\} + s_1^2 - dt_1^2 \\ &= k\{s_1(a_2 - a_1) - dt_1(b_2 - b_1) + 1\} \\ &= kx_1 \end{aligned}$$

同様に、

$$s_1 t_2 - s_2 t_1 = ky_1$$

となる。ここで $x_1$ も $y_1$ も整数。

いま $y_1 \neq 0$ である。なぜなら、$y_1 = 0$ とすると、

$$ky_1 = s_1 t_2 - s_2 t_1 = 0$$

となり、

$$\frac{s_1}{t_1} = \frac{s_2}{t_2}$$

であり矛盾。

等式 (15) と (16) より、

$$(s_1 - \alpha t_1)(s_2 + \alpha t_2) = kx_1 + \alpha k y_1 = k(x_1 + \alpha y_1) \tag{17}$$

$$(s_1 + \alpha t_1)(s_2 - \alpha t_2) = kx_1 - \alpha k y_1 = k(x_1 - \alpha y_1) \tag{18}$$

が得られる。(13) と (14) を掛け合わせると (17), (18) より、

$$\begin{aligned} k^2 &= (s_1^2 - dt_1^2)(s_2^2 - dt_2^2) \\ &= (s_1 - \alpha t_1)(s_2 + \alpha t_2)(s_1 + \alpha t_1)(s_2 - \alpha t_2) \\ &= k^2(x_1 + \alpha y_1)(x_1 - \alpha y_1) \\ &= k^2(x_1^2 - dy_1^2) \end{aligned}$$

よって、

$$x_1^2 - dy_1^2 = 1$$

つまり $(x_1, y_1)$ は方程式 (1) の非自明な解となり矛盾。

## 4 解の行列表示

この節では、一般化されたペルの方程式

$$x^2 - dy^2 = m^2$$

の解の行列表示を考える。まず、最小解 $(a, b)$ に対し、

$$\begin{aligned} x_n &= \frac{m}{2}\left\{\left(\frac{a}{m}+\frac{b}{m}\sqrt{d}\right)^n + \left(\frac{a}{m}-\frac{b}{m}\sqrt{d}\right)^n\right\} \\ y_n &= \frac{m}{2\sqrt{d}}\left\{\left(\frac{a}{m}+\frac{b}{m}\sqrt{d}\right)^n + \left(\frac{a}{m}-\frac{b}{m}\sqrt{d}\right)^n\right\} \end{aligned}$$

とおくと、$(x_n, y_n)$ はこの方程式の一般解となる。

$$A = \frac{1}{m}\begin{pmatrix} a & db \\ b & a \end{pmatrix}$$

とおくと、

$$|A| = \frac{1}{m^2}(a^2 - db^2) = \frac{m^2}{m^2} = 1$$

であり、

$$\begin{pmatrix} x_n \\ y_n \end{pmatrix} = A^n \begin{pmatrix} m \\ 0 \end{pmatrix}$$

とおくと、方程式の一般解は $(\pm x_n, \pm y_n)$ である。

**例 10** $m = 1$, $d = 3$ のとき、$(2,1)$, $(7,4)$, $(26,15)$, $(97,56)$, $(362,209)$, $(1351,780)$, $\cdots$ は解である。

## 参考文献

[1] 倉田令二朗. ガウス 2 次形式論 (1). 河合ブックレット　数学シリーズ 3. 河合文化教育研究所, 1987.

[2] ゲリファント. 方程式の解き方. 東京図書, 1993.